Experience with Firewalls and IPsec

Moderator: Stephen Kent (GTE Internetworking)

Panelists: Naganand Doraswamy (Bay Networks),
Cheryl Madson (Cisco), and Dan McDonald (Sun)

Abstract

This panel will provide a status update on IPsec, the IETF standard for Internet layer security, including preliminary experiences with the testing and deployment of IPsec in both router/firewall and end system (host) environments. The final, standard versions of the IPsec traffic security protocols will be described briefly to provide a background for the panel discussion. The three panelists assembled for this discussion are all implementers of IPsec for major vendors. They will discuss their experience in developing and deploying this new technology to create secure Virtual Private Networks (VPNs), provide mobile user security, etc.

IPsec

The term IPsec refers to a set of protocols developed under the auspices of the Internet Engineering Task Force (IETF) to provide security for IP layer traffic, for both IPv4 and IPv6. In fact, compliant implementations of IPv6 require support of IPsec, underscoring the IETF's commitment to improving IP security in the Internet. IPsec protocols can be employed between a pair of end systems (hosts), between a pair of security gateways (e.g., firewalls), or between an end system and a security gateway. In the context of a host, the IPsec implementation may be integrated into the IP stack, or may be retrofitted as a "bump-in-the-stack" module. IPsec also may be implemented in stand-alone, "bump-in-the-wire" devices for use with hosts or gateways. This implementation option flexibility allows users and system administrators to select differing points at which to deploy IPsec, in support of varying security requirements and to support incremental deployment.

Included in IPsec are two protocols used to protect IP traffic (AH and ESP), plus a security association (SA) and key management protocol (ISAKMP). AH, the Authentication Header, provides connectionless integrity, data origin authentication, and optional partial sequence integrity (anti-replay) for the payload of an IP datagram, plus selected portions of the IP header. ESP, the Encapsulating Security Payload, provides confidentiality for an IP payload. ESP may provide connectionless integrity, data origin authentication, and optional partial sequence integrity (anti-replay) as well, for the payload. ISAKMP, the Internet Security Association and Key Management Protocol, is used to establish security associations for AH and ESP, including per-association keys, and other security parameters needed to ensure appropriate processing of IPsec-protected traffic.

AH and ESP can be applied directly to IP traffic, or to traffic within IP tunnels. The former means of employing AH and ESP is referred to as "transport mode," while the latter is characterized as "tunnel mode." An SA between a pair of hosts may be either transport or tunnel mode, though the former is more common than the latter. An SA terminating at a security gateway is always in tunnel mode, to permit the decapsulated traffic to traverse the gateway enroute to its final destination. (The exception to this general rule arises if the target of the SA is a host function within the gateway.) A transport mode IPsec SA may be encapsulated by a tunnel mode SA (e.g., to provide end-to-end security for traffic that traverses a security gateway enroute to a host or server "behind" that gateway).

Although IPsec is conceptually simple, in practice, implementations may be quite complex. This is especially true at gateways, where the primary information available to the IPsec implementation for making processing decisions is that which can be gleaned from the IP headers of packets traversing the gateway. Providing SAs at variable granularity and dealing with processing of ICMP messages (e.g., especially ICMP PMTU messages) further complicates the task of producing a secure, high performance IPsec implementation.

These panelists have experience in the trials and tribulations of developing IPsec implementations for host and gateway environments and will share these experiences with the audience.